II. LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (**Currently Amended**) A method for managing network access of a computing device, which is capable of communicating via one or more networks, where trusted enforcement of the access occurs at the device, comprising the steps of:

providing software adapted to be installed in the device, the software configured to communicate with a **secure tamper-resistant physical** token operatively coupled to**, local to and removably attachable to** the device;

storing a network access parameter in memory of ~~**a tamper-resistant**~~ **said** secure **tamper-resistant physical** token ~~**capable of being operatively coupled to said device**~~, said network access parameter being associated with a first network, said **secure tamper-resistant physical** token ~~**local to and removably attachable to said device, said token**~~ comprising a processor configured to execute an application, said application configured to determine if said network access parameter has been met or exceeded; and

granting the device access to the first network if the application determines that the network access parameter has not been met or exceeded.

2. (Previously Presented) The method of claim 1, wherein said network access parameter is selected from the group consisting of: maximum number of connections to said first network, time of day, period of time, day in week, date, range of dates, maximum period of time spent connected to said first network, device address, subnet ID, and LAN ID.

3. (Previously Presented) The method of claim 1, further comprising the step of storing one or more additional network access parameters in said secure token.

4. (Previously Presented) The method of claim 3, further comprising the steps of:

determining if said one or more additional access parameters have been met or exceeded and

denying access to said first network if any of said network access parameters have been met or exceeded.

5. (Previously Presented) The method of claim 3, further comprising the steps of:

determining if said one or more additional access parameters have been met and

restricting access to a portion of said first network if any of said network access parameters have been met or exceeded.

6. (Previously Presented) The method of claim 5, wherein said portion of said first network includes a server and said method further comprising the steps of:

authorizing additional usage of said first network at said server and

modifying said network access parameter.

7. (Previously Presented) The method of claim 6, wherein said step of authorizing comprises the step of receiving payment for said additional usage of said first network.

8. (Previously Presented) The method of claim 3, further comprising the step of

determining if said one or more additional access parameters has been met and

allowing access to said first network if all of said network access parameters have not been met.

9. (Previously Presented) The method of claim 3, wherein at least one of said additional network access parameters is associated with a second network.

10. (Previously Presented) The method of claim 1, wherein said first network is an 802.11 network.

11. (Previously Presented) The method of claim 10, wherein said secure token is implemented through a USB adapter.

12. (Original) The method of claim 10, wherein current time is received from an access point on said 802.11 network.

13. (Cancelled)

14. (Cancelled)

15. (Previously Presented) The method of claim 1, wherein said secure token is unique to said device.

16. (Previously Presented) The method of claim 1, wherein said secure token comprises authentication information for authenticating said device with said network.

17. (Previously Presented) The method of claim 1, wherein said network access parameter is pre-stored within said secure token.

18. (**Currently Amended**) A system for managing network access of a computing device, which is capable of communicating via one or more networks, where trusted enforcement of the access occurs at the device, the system comprising:

~~**software adapted to be installed in the device, the software configured to communicate with a token operatively coupled to the device; and**~~

a secure tamper-resistant physical token **operatively coupled to,** local to and removably attachable to the device**; and**

software adapted to be installed in the device, the software configured to communicate with said secure tamper-resistant physical token, said physical token comprising:

a communications interface for communicating data to and from said physical token;

a storage including at least one access parameter associated with a first network; and

a processor configured to execute an application, said application configured to determine if said access parameter has been met or exceeded, whereby the device is granted access to the first network if said access parameter has not been met or exceeded.

19. (Previously Presented) The system of claim 18, wherein said at least one access parameter is part of a first usage plan for said first network.

20. (Previously Presented) The system of claim 19, wherein said storage further includes a usage application for tracking and enforcing usage of said first network according to said first usage plan.

21. (Previously Presented) The system of claim 18, further comprising an adapter for connecting said physical token to a device capable of communicating with said first network.

22. (Previously Presented) The system of claim 18, wherein said storage further includes at least one access parameter associated with a second network.

23. (Previously Presented) The system of claim 18, wherein said storage further includes authentication information for authenticating said device with said first network.